全球服务器证书SSL配置手册

Tomcat 4.1

北京数字证书认证中心

BEIJING CERTIFICATE AUTHORITY

目 录

1 开始申请之前需要注意......3
2 如何产生私钥......3
3 CSR生成指南......5
4 证书安装指南......6
5 如何配置SSL......12
6 启动和停止Tomcat......13
7 验证SSL连接......13
8 灾难恢复......13

1 开始申请之前需要注意

需要安装服务器软件并配置环境，下面我们以 Keytool 和 Tomcat 为例进行说明：

a) 首先需要准备所需的软件：

- Java(TM) 2 SDK, Standard Edition 1.4.1_01

  下载 j2sdk-1_4_1_01-windows-i586.exe

- Tomcat 4.1

  下载 tomcat-4.1.18.exe

- Windows 2000 SP 2 or Windows NT SP6a
- Tomcat 做为单独的服务器

b) 环境变量设置为：

Variable	**Value**	**User Name**
CATALINA_HOME	C:\Tomcat~1.1	[SYSTEM]
JAVA_HOME	C:\j2sdk1.4.1_01	[SYSTEM]
JSSE_HOME	C:\j2sdk1.4.1_01\jre\lib\ext	[SYSTEM]
TOMCAT_HOME	C:\Tomcat~1.1	[SYSTEM]
Path	C:\j2sdk1.4.1_01\bin	Administrator

c) 测试服务器

安装完 Tomcat，并配置完环境后，启动 Tomcat 并进行测试：

http://localhost:8080 to make sure http is working

如果没有问题，我们可以进行下一步操作了。

2 如何产生私钥

新打开一个 DOS 窗口：

1) 新建一个本地的证书密钥存储（Certificate keystore）

keytool -genkey -alias tomcat -keyalg RSA \ -keystore

请注意:

! 当 keystore 建立后，需要指定 keystore 的存储位置

! 如果更新证书，你必须重新创建一个新的密钥对和 keystore

! 当您生成 CSR 或安装自签的 keystore 证书时，请使用相同的别名

例如:

C:\>keytool -genkey -alias myalias -keyalg RSA -keystore c:\.mykeystore

Enter keystore password: 输入 keystore 口令，如 password

What is your first and last name?

[Unknown]: 输入通用名，如 www.bjca.org.cn

What is the name of your organizational unit?

[Unknown]: 输入部门名称，如 Sales Dept

What is the name of your organization?

[Unknown]: 输入您的组织名称，如 Beijing Certificate Authority

What is the name of your City or Locality?

[Unknown]: 输入您所在的市/县/区，如 Beijing

What is the name of your State or Province?

[Unknown]: 输入您所在的省/自治区/直辖市，如 Beijing

What is the two-letter country code for this unit?

[Unknown]: 输入您所在国家的 ISO 国家代码，中国为 CN

is CN=www.bjca.org.cn, OU=Sales Dept, O=Beijing Certificate Authority, L=Beijing, ST=Beijing, C=CN correct?

[no]: yes

Enter key password for (RETURN if same as keystore password): 输入密钥口令

The same password MUST be used.

非常重要: Tomcat will recognize the location of this keystore even if the specified attributes in your server.xml point to a different keystore.

C:\>

2) 确认 keystore 建立成功

例如:

C:\>keytool -list -v -keystore c:\.mykeystore

Enter keystore password: password

Keystore type: jks

Keystore provider: SUN

Your keystore contains 1 entry

Alias name: myalias

Creation date: Jan 8, 2003

Entry type: keyEntry

Certificate chain length: 1

Certificate[1]:

Owner: CN=www.bjca.org.cn, OU=Sales Dept, O=Beijing Certificate Authority, L=Beijing, ST=Beijing, C=CN

Issuer: CN=www.bjca.org.cn, OU=Sales Dept, O=Beijing Certificate Authority, L=Beijing, ST=Beijing, C=CN

Serial number: 3e1cd4e9

Valid from: Wed Jan 08 20:48:25 EST 2003 until: Tue Apr 08 21:48:25 EDT 2003

Certificate fingerprints:

MD5: D0:BA:7C:A4:D1:D9:CF:46:38:E5:48:22:8E:AB:E2:9B

SHA1: 4A:33:FA:11:D6:5F:F4:73:9D:7A:2B:E2:89:F8:C3:57:69:0C:DC:7E

3 CSR生成指南

1) 按照如下方法生成 CSR

keytool -certreq -keyalg RSA -alias tomcat -file certreq.csr \ -keystore

重要提示:

! 当您生成 CSR 或安装自签的 keystore 证书时，请使用相同的别名

例如:

C:\>keytool -certreq -keyalg RSA -alias myalias -file certreq.txt -keystore c:\.mykeystore

Enter keystore password: password

C:\>

2) 生成的 CSR 如下:

-----BEGIN NEW CERTIFICATE REQUEST-----

MIIBujCCASMCAQAwejELMAkGA1UEBhMCQ0ExEDAOBgNVBAgTB09udGFyaW8xDz

ANBgNVBAcTBk90

dGF3YTEQMA4GA1UEChMHRW50cnVzdDETMBEGA1UECxMKRW50cnVzdCBDUzEh

MB8GA1UEAxMYd3d3

5w6T+q/f+wIDAQABoAAwDQYJKoZIhvcNAQEEBQADgYEAF+0hqAqXumz/vGrzGVhKH

lnxd7HW3ezS

GIbIUcOy1YdDc/1ZCqRpu3utYIZ6welK++l+QjlbL6p5RJJETkkLKXjb/WVFajNuPl7Yob9p

bwA7

JBrCCKbFj+kzDNbGhCR1RgFA9vQj5vob41Vj+k+TQchliuTLL9rFXNDHrtgTMtA=

-----END NEW CERTIFICATE REQUEST-----

4 证书安装指南

按照如下方法安装 BJCA 的 SSL 证书

1) 安装 SSL 证书和证书链

输入命令:

keytool -import -alias root -keystore your_keystore_filename \ -trustcacerts -file filename_of_the_combined_chain_and_webcert

例如: C:\>keytool -import -alias myalias -keystore c:\.mykeystore -trustcacerts -file c:\webcert.txt

由于 java 把“cacerts”文件看作可信任的根 CA，如果根证书已经存在，则不必再将证书链导入“cacerts”。

例如:

-----BEGIN CERTIFICATE-----

MIIC4zCCAkygAwIBAgIBAzANBgkqhkiG9w0BAQUFADBFMQswCQYDVQQGEwJVUzE

Y

MBYGA1UEChMPR1RFIENvcnBvcmF0aW9uMRwwGgYDVQQDExNHVEUgQ3liZXJUc

nVz

dCBSb290MB4XDTAxMDgyMTIwMDIwOVoXDTA2MDEwMTIzNTkwMFowgcMxCzAJBg

NV

BAYTAlVTMRQwEgYDVQQKEwtFbnRydXN0Lm5ldDE7MDkGA1UECxMyd3d3LmVudH

J1

c3QubmV0L0NQUyBpbmNvcnAuIGJ5IHJlZi4gKGxpbWl0cyBsaWFiLikxJTAjBgNV

BAsTHChjKSAxOTk5IEVudHJ1c3QubmV0IExpbWl0ZWQxOjA4BgNVBAMTMUVudHJ1

Ct8k2pzWUHmBelrTN/fCStgpkiZk0eSYbDoAivU0m2X47eMQ//24SVjcoN6COWuB

sRYZYblUtuZDAgEDo2YwZDAPBgNVHRMECDAGAQH/AgEDMA4GA1UdDwEB/wQEA

wIB

BjBBBgNVHR8EOjA4MDagNKAyhjBodHRwOi8vY2RwLmJhbHRpbW9yZS5jb20vY2dp

LWJpbi9DUkwvR1RFUm9vdC5jZ2kwDQYJKoZIhvcNAQEFBQADgYEAgbZwffFU+Fjj

NYTSoUFyRAAysIauOknVaLteQPQJxBGLMhXGdfejVBTWLb1UTFBQXNNCiqm8Co+d

YikuVB+0/1habRkb+k4vFe6tn5IvQMnfhZbSJNoXn5IlGVDWQYlfC0/R1wjfv+U6

rzTJbJ7WXX0Ka5jKLKuckXNvu7EqOA4=

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

MIIGEjCCBXugAwIBAgIEN0w5HDANBgkqhkiG9w0BAQQFADCBwzELMAkGA1UE

BhMCVVMxFDASBgNVBAoTC0VudHJ1c3QubmV0MTswOQYDVQQLEzJ3d3cuZW50

cnVzdC5uZXQvQ1BTIGluY29ycC4gYnkgcmVmLiAobGltaXRzIGxpYWIuKTEl

MCMGA1UECxMcKGMpIDE5OTkgRW50cnVzdC5uZXQgTGltaXRlZDE6MDgGA1UE

AxMxRW50cnVzdC5uZXQgU2VjdXJlIFNlcnZlciBDZXJ0aWZpY2F0aW9uIEF1

dGhvcml0eTAeFw0wMzAxMDkxNzE4MjFaFw0wMzExMTAxNzQ2NDFaMHoxCzAJ

BgNVBAYTAkNBMRAwDgYDVQQIEwdPbnRhcmlvMQ8wDQYDVQQHEwZPdHRhd2Ex

EDAOBgNVBAoTB0VudHJ1c3QxEzARBgNVBAsTCkVudHJ1c3QgQ1MxITAfBgNV

BAMTGHd3dy50ZXN0Y2VydGlmaWNhdGVzLmNvbTCBnzANBgkqhkiG9w0BAQEF

MCfPxacCAwEAAaOCA1kwggNVMAsGA1UdDwQEAwIFoDArBgNVHRAEJDAigA8y

BAMCBkAwEwYDVR0lBAwwCgYIKwYBBQUHAwEwggFoBgNVHSAEggFfMIIBWzCC

AVcGCSqGSIb2fQdLAjCCAUgwJgYIKwYBBQUHAgEWGmh0dHA6Ly93d3cuZW50

cnVzdC5uZXQvY3BzMIIBHAYIKwYBBQUHAgIwggEOGoIBClRoZSBFbnRydXN0
IFNTTCBXZWIgU2VydmVyIENlcnRpZmljYXRpb24gUHJhY3RpY2UgU3RhdGVt
ZW50IChDUFMpIGF2YWlsYWJsZSBhdCB3d3cuZW50cnVzdC5uZXQvY3BzICBp
IGJ5IHJlZi4gKGxpbWl0cyBsaWFiLikxJTAjBgNVBAsTHChjKSAxOTk5IEVu
dHJ1c3QubmV0IExpbWl0ZWQxOjA4BgNVBAMTMUVudHJ1c3QubmV0IFNlY3Vy
ZSBTZXJ2ZXIgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkxDjAMBgNVBAMTBUNS
TDU2MCygKqAohiZodHRwOi8vd3d3LmVudHJ1c3QubmV0L0NSTC9zZXJ2ZXIx
LmNybDAfBgNVHSMEGDAWgBTwF2ITVT2z/woAa/tQhJfz7WLQGjAdBgNVHQ4E
FgQU8PAQJvkXpS82OTYbatZ36ZPmzM4wCQYDVR0TBAIwADAZBgkqhkiG9n0H
QQAEDDAKGwRWNS4wAwIDKDANBgkqhkiG9w0BAQQFAAOBgQCviVPHpMdBNRc+
J88+VVW8k3bQQlyIsbtBr3XYDkqS5o9tSXXmpwJU6G40StrObPdKLHI2C+ho
GiXnmXjFlKXPe/pOjHnU3azNBPJR7edrp523EB0muGTadk9rhnoRNEpUAw9u
hgdRmxjwjO0XhBLVPcsCiiyFoDZpaU9o3MHVXQ==
-----END CERTIFICATE-----

您必须接受这个可信的 CA。

您应该收到这样的信息："Certificate Reply Was Installed Into Keystore"

如果在 UNIX 环境下，以上的例子是颠倒的。

2)　在 SUN JAVA 1.4.1 或更低版本上安装 SSL 证书

输入命令：

keytool -import -alias root -keystore \ -trustcacerts –file

！注意：当您生成 CSR 或安装自签的 keystore 证书时，请使用相同的别名

例如：

C:\>keytool -import -alias myalias -keystore c:\.mykeystore -trustcacerts -file c:\webcert.txt

由于 java 把“cacerts”文件看作可信任的根 CA，Entrust 的根证书没有预埋到 java 1.4.x 或更低版本中，不必将证书链导入“cacerts”。

例如：

-----BEGIN CERTIFICATE-----

MIIE2DCCBEGgAwIBAgIEN0rSQzANBgkqhkiG9w0BAQUFADCBwzELMAkGA1UEBhM
C
VVMxFDASBgNVBAoTC0VudHJ1c3QubmV0MTswOQYDVQQLEzJ3d3cuZW50cnVzdC
5u
ZXQvQ1BTIGluY29ycC4gYnkgcmVmLiAobGltaXRzIGxpYWIuKTElMCMGA1UECxMc
KGMpIDE5OTkgRW50cnVzdC5uZXQgTGltaXRlZDE6MDgGA1UEAxMxRW50cnVzdC5u
ZXQgU2VjdXJlIFNlcnZlciBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAeFw05OTA1
MjUxNjA5NDBaFw0xOTA1MjUxNjM5NDBaMIHDMQswCQYDVQQGEwJVUzEUMBIGA
1UE
ChMLRW50cnVzdC5uZXQxOzA5BgNVBAsTMnd3dy5lbnRydXN0Lm5ldC9DUFMgaW5j
b3JwLiBieSByZWYuIChsaW1pdHMgbGlhYi4pMSUwIwYDVQQLExwoYykgMTk5OSBF
bnRydXN0Lm5ldCBMaW1pdGVkMTowOAYDVQQDEzFFbnRydXN0Lm5ldCBTZWN1cm
Ug
U2VydmVyIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MIGdMA0GCSqGSIb3DQEBAQUA
A4GLADCBhwKBgQDNKIM0VBuJ8w+vN5Ex/68xYMmo6LIQaO2f55M28Qpku0f1BBc/
I0dNxScZgSYMVHINiC3ZH5oSn7yzcdOAGT9HZnuMNSjSuQrfJNqc1lB5gXpa0zf3
wkrYKZImZNHkmGw6AIr1NJtl+O3jEP/9uElY3KDegjlrgbEWGWG5VLbmQwIBA6OC
AdcwggHTMBEGCWCGSAGG+EIBAQQEAwIABzCCARkGA1UdHwSCARAwggEMMIH
eoIHb
oIHYpIHVMIHSMQswCQYDVQQGEwJVUzEUMBIGA1UEChMLRW50cnVzdC5uZXQxO
zA5
BgNVBAsTMnd3dy5lbnRydXN0Lm5ldC9DUFMgaW5jb3JwLiBieSByZWYuIChsaW1p
dHMgbGlhYi4pMSUwIwYDVQQLExwoYykgMTk5OSBFbnRydXN0Lm5ldCBMaW1pdGV
k
MTowOAYDVQQDEzFFbnRydXN0Lm5ldCBTZWN1cmUgU2VydmVyIENlcnRpZmljYXR
p
b24gQXV0aG9yaXR5MQ0wCwYDVQQDEwRDUkwxMCmgJ6AlhiNodHRwOi8vd3d3Lm
Vu
dHJ1c3QubmV0L0NSTC9uZXQxLmNybDArBgNVHRAEJDAigA8xOTk5MDUyNTE2MDk
0

MFqBDzIwMTkwNTI1MTYwOTQwWjALBgNVHQ8EBAMCAQYwHwYDVR0jBBgwFoAU

8Bdi

E1U9s/8KAGv7UISX8+1i0BowHQYDVR0OBBYEFPAXYhNVPbP/CgBr+1CEl/PtYtAa

MAwGA1UdEwQFMAMBAf8wGQYJKoZIhvZ9B0EABAwwChsEVjQuMAMCBJAwDQYJK

oZI

hvcNAQEFBQADgYEAkNwwAvpkdMKnCqV8IY00F6j7Rw7/JXyNEwr75Ji174z4xRAN

95K+8cPV1ZVqBLssziY2ZcgxxufuP+NXdYR6Ee9GTxj005i7qIcyunL2POI9n9cd

2cNgQ4xYDiKWL2KjLB+6rQXvqzJ4h6BUcxm1XAX5Uj5tLUUL9wqT6u0G+bI=

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

MIIGEjCCBXugAwIBAgIEN0w5HDANBgkqhkiG9w0BAQQFADCBwzELMAkGA1UE

BhMCVVMxFDASBgNVBAoTC0VudHJ1c3QubmV0MTswOQYDVQQLEzJ3d3cuZW50

cnVzdC5uZXQvQ1BTIGluY29ycC4gYnkgcmVmLiAobGltaXRzIGxpYWIuKTEl

MCMGA1UECxMcKGMpIDE5OTkgRW50cnVzdC5uZXQgTGltaXRlZDE6MDgGA1UE

AxMxRW50cnVzdC5uZXQgU2VjdXJlIFNlcnZlciBDZXJ0aWZpY2F0aW9uIEF1

dGhvcml0eTAeFw0wMzAxMDkxNzE4MjFaFw0wMzExMTAxNzQ2NDFaMHoxCzAJ

BgNVBAYTAkNBMRAwDgYDVQQIEwdPbnRhcmlvMQ8wDQYDVQQHEwZPdHRhd2Ex

EDAOBgNVBAoTB0VudHJ1c3QxEzARBgNVBAsTCkVudHJ1c3QgQ1MxITAfBgNV

BAMTGHd3dy50ZXN0Y2VydGlmaWNhdGVzLmNvbTCBnzANBgkqhkiG9w0BAQEF

MCfPxacCAwEAAaOCA1kwggNVMAsGA1UdDwQEAwIFoDArBgNVHRAEJDAigA8y

BAMCBkAwEwYDVR0lBAwwCgYIKwYBBQUHAwEwggFoBgNVHSAEggFfMIIBWzCC

AVcGCSqGSIb2fQdLAjCCAUgwJgYIKwYBBQUHAgEWGmh0dHA6Ly93d3cuZW50

cnVzdC5uZXQvY3BzMIIBHAYIKwYBBQUHAgIwggEOGoIBClRoZSBFbnRydXN0

IFNTTCBXZWIgU2VydmVyIENlcnRpZmljYXRpb24gUHJhY3RpY2UgU3RhdGVt

ZW50IChDUFMpIGF2YWlsYWJsZSBhdCB3d3cuZW50cnVzdC5uZXQvY3BzICBp

IGJ5IHJlZi4gKGxpbWl0cyBsaWFiLikxJTAjBgNVBAsTHChjKSAxOTk5IEVu

dHJ1c3QubmV0IExpbWl0ZWQxOjA4BgNVBAMTMUVudHJ1c3QubmV0IFNlY3Vy

ZSBTZXJ2ZXIgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkxDjAMBgNVBAMTBUNS

TDU2MCygKqAohiZodHRwOi8vd3d3LmVudHJ1c3QubmV0L0NSTC9zZXJ2ZXIx

LmNybDAfBgNVHSMEGDAWgBTwF2ITVT2z/woAa/tQhJfz7WLQGjAdBgNVHQ4E

FgQU8PAQJvkXpS82OTYbatZ36ZPmzM4wCQYDVR0TBAIwADAZBgkqhkiG9n0H

QQAEDDAKGwRWNS4wAwIDKDANBgkqhkiG9w0BAQQFAAOBgQCviVPHpMdBNRc+

J88+VVW8k3bQQlyIsbtBr3XYDkqS5o9tSXXmpwJU6G40StrObPdKLHI2C+ho

GiXnmXjFlKXPe/pOjHnU3azNBPJR7edrp523EB0muGTadk9rhnoRNEpUAw9u

hgdRmxjwjO0XhBLVPcsCiiyFoDZpaU9o3MHVXQ==

-----END CERTIFICATE-----

您需要接受这个可信 CA。

Enter keystore password: password

Top-level certificate in reply:

Owner: CN=Entrust.net Secure Server Certification Authority, OU=(c) 1999 Entrust .net Limited, OU=www.entrust.net/CPS incorp. by ref. (limits liab.), O=Entrust.n et, C=US

Issuer: CN=Entrust.net Secure Server Certification Authority, OU=(c) 1999 Entrus t.net Limited, OU=www.entrust.net/CPS incorp. by ref. (limits liab.), O=Entrust. net, C=US

Serial number: 374ad243

Valid from: Tue May 25 12:09:40 EDT 1999 until: Sat May 25 12:39:40 EDT 2019

Certificate fingerprints:

  MD5: DF:F2:80:73:CC:F1:E6:61:73:FC:F5:42:E9:C5:7C:EE

  SHA1: 99:A6:9B:E6:1A:FE:88:6B:4D:2B:82:00:7C:B8:54:FC:31:7E:15:39

... is not trusted. Install reply anyway? [no]: yes

证书已经装入 keystore。

如果在 UNIX 环境下，以上的例子是颠倒的。

3)　在 SUN JAVA 1.4.2 或更高版本上安装 SSL 证书

输入命令：keytool -import -alias ralias -keystore your_keystore_filename

!请注意：当您生成 CSR 或安装自签的 keystore 证书时，请使用相同的别名

例如：

C:\>PROGRA~1\JAVA\J2RE14~1.2_0\BIN>keytool -import -alias ralias -keystore c:\15keystore -trustcacerts -file c:\certnoroot.txt

Enter keystore password: password

您将收到这样的信息:

"Certificate Reply Was Installed Into Keystore"

5 如何配置SSL

1) 设置 server.xml 文件，举例如下:

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on Port 8443 -->

    <Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
    port="443" minProcessors="5" maxProcessors="75" enableLookups="true"
    acceptCount="100" debug="0" scheme="https" secure="true"
    useURIValidationHack="false" disableuploadTimeout="true">

  <Factory className="org.apache.coyote.tomcat4.CoyoteServerSocketFactory"
    clientAuth="false" protocol="TLS" keystoreFile="C:\.mykeystore"
    keystorePass="password" />

  </Connector>
```

2) 启动 Tomcat

从“开始”菜单或命令行进入 Tomcat 的 Bin 目录，输入 Startup.bat 或 Catalina run 启动 Tomcat。

通过输入https://locahost，确认您是否能够使用自签发的证书。

输入https://localhost/admin/index.jsp，进入Tomcat管理员界面。

在 Tomcat 的独立服务界面点击 443 链接，确认您正在使用 keystore 的位置和您指定的文件名。

Keystore 文件名为: C:\.mykeystore

现在您可以开始申请 BJCA 的全球服务器证书了。

6 启动和停止Tomcat

从“开始”菜单或命令行进入 Tomcat 的 Bin 目录，输入 Startup.bat 或 Catalina run 启动 Tomcat。

7 验证SSL连接

启动Tomcat，输入https://localhost:端口号，如在server.xml文件中设置端口为 443，如下所示：

https://localhost

the browser will assume port 443

8 灾难恢复

找到包含密钥对的 keystore 文件。

将 keystore 文件备份到移动介质或保存到硬盘中一个安全的地方，以便恢复系统。